

# A problem related to the divisibility of exponential sums

Xiaogang Liu

## Abstract

Francis Castro, et al computed the exact divisibility of families of exponential sums associated to binomials  $F(X) = aX^{d_1} + bX^{d_2}$  over  $\mathbb{F}_p$ , and a conjecture is presented for related work. Here we study this question.

## I. INTRODUCTION

Exponential sums and their divisibility have been applied to characterize important properties of objects in applied mathematics. Good estimates for the divisibility of exponential sums exist [1], [3], [4], [5]. In [2], the authors investigated the exact divisibility of exponential sums associated to polynomials in one variable over the prime field  $\mathbb{F}_p$ . It is difficult in general, and they computed the exact divisibility of families of exponential sums associated to binomials  $F(X) = aX^{d_1} + bX^{d_2}$ , when  $a, b \in \mathbb{F}_p^*$ .

Let  $\mathbb{Q}_p$  be the  $p$ -adic field,  $\xi$  be a primitive  $p$ -th root of unity in  $\overline{\mathbb{Q}_p}$ , define  $\theta = 1 - \xi$  and denote by  $\nu_\theta$  the valuation over  $\theta$ . Note that  $\nu_\theta(p) = p - 1$  and  $\nu_p(x) = \frac{\nu_\theta(x)}{p-1}$ . Let  $\phi : \mathbb{F}_p \rightarrow \mathbb{Q}(\xi)$  be a nontrivial additive character. The exponential sum associated to  $F(X) = \sum_{i=1}^N a_i X^{d_i}$  is defined as

$$S_p(F) = \sum_{x \in \mathbb{F}_p} \phi(F(x)).$$

A bound is presented for the valuation of an exponential sum with respect to  $\theta$ .

*Theorem 1:* ([4]) Let  $F(X) = \sum_{i=1}^N a_i X^{d_i}$ ,  $a_i \neq 0$ . If  $S_p(F)$  is the exponential sum  $\sum_{x \in \mathbb{F}_p} \phi(F(x))$ , then  $\nu_\theta(S_p(F)) \geq \mu_p(d_1, \dots, d_N)$ , where

$$\mu_p(d_1, \dots, d_N) = \min_{(j_1, \dots, j_N)} \left\{ \sum_{i=1}^N j_i \mid 0 \leq j_i < p \right\},$$

for  $(j_1, \dots, j_N) \neq (0, \dots, 0)$  a solution to the modular equation

$$d_1 j_1 + d_2 j_2 + \dots + d_N j_N \equiv 0 \pmod{p-1}.$$

.....

The author is with Department of Computer Science and Engineering, Nanjing University of Technology, Nanjing 211800, PR China e-mail: liuxg0201@njtech.edu.cn.

For the binomial case, the authors made the following conjecture [2]

$$\mu_p(d_1, d_2) \leq \frac{p-1}{2}, \quad (1)$$

and we will investigate this problem in this correspondence.

## II. MAIN RESULT

*Theorem 2:* Let  $1 \leq d_1 \neq d_2 \leq p-2$  be positive integers, and  $p \geq 5$  is a prime, then inequality (1) holds.

*Proof:* First we consider the case when  $d_1, d_2$  are odd numbers, and  $\gcd(d_1, p-1) = \gcd(d_2, p-1) = 1$ .

Let  $i = 1$ , then  $d_1 i + d_2 j = d_1 + d_2 j$ . If it is zero modular  $p-1$ , then  $j \neq p-1$ ; if  $j = p-2$  then  $d_1 + d_2 j = d_1 + d_2(p-2) = d_1 + d_2(p-1) - d_2$  doesn't equal to zero modular  $p-1$ . Also,  $j \neq 0$ . So, we have

$$1 \leq j \leq p-3. \quad (2)$$

If  $j > \frac{p-1}{2}$ , let's consider the following sets

$$\left[1 - \frac{1}{2^{k-1}}, 1 - \frac{1}{2^k}\right)$$

for  $k = 1, 2, 3, \dots$ . We can find that the union of the sets is  $[0, 1)$ . Let's assume that  $j = \alpha_{k-1}(p-1)$  and  $\alpha_{k-1} \in \left[1 - \frac{1}{2^{k-1}}, 1 - \frac{1}{2^k}\right)$ , then

$$\begin{aligned} 1 - \frac{1}{2^{k-1}} \leq \alpha_{k-1} &\implies \left(1 - \frac{1}{2^{k-1}}\right)(p-1) \leq p-3 \text{ (equ:2)} \\ \implies p-1 - (p-3) &\leq \frac{p-1}{2^{k-1}} \implies 2 \leq \frac{p-1}{2^{k-1}} \implies 2^k \leq p-1 \implies \frac{p-1}{2} \geq 2^{k-1}. \end{aligned} \quad (3)$$

Since  $d_1 + d_2 j \equiv 0 \pmod{p-1}$ , we have

$$d_1 \cdot 2 + d_2 \cdot 2j \equiv 0 \pmod{p-1}$$

and,  $2j \in 2 \left[1 - \frac{1}{2^{k-1}}, 1 - \frac{1}{2^k}\right)(p-1) = \left[2 - \frac{1}{2^{k-2}}, 2 - \frac{1}{2^{k-1}}\right)(p-1) = p-1 + \left[1 - \frac{1}{2^{k-2}}, 1 - \frac{1}{2^{k-1}}\right)(p-1)$ . So, we can assume

$$2j \equiv j_{k-2} \pmod{p-1}$$

and  $j_{k-2} \in \left[1 - \frac{1}{2^{k-2}}, 1 - \frac{1}{2^{k-1}}\right)(p-1)$ . Let  $j_{k-1} = j$ . We have

$$d_1 \cdot 2 + d_2 \cdot j_{k-2} \equiv 0 \pmod{p-1}$$

multiply both sides of the modular equation by 2 again, and proceed in this way, we find that

$$d_1 \cdot 2^{k-1} + d_2 \cdot j_0 \equiv 0 \pmod{p-1}$$

and  $j_0 \in \left[0, \frac{1}{2}\right)(p-1)$ . So,  $i' = 2^{k-1}, j' = j_0 \in \left[0, \frac{p-1}{2}\right]$  (equ: 3). If  $i' + j' \leq \frac{p-1}{2}$ , the process is done. Otherwise, we let

$$i'' = \frac{p-1}{2} - i', j'' = \frac{p-1}{2} - j'$$

then

$$\begin{aligned}
d_1 \cdot i'' + d_2 \cdot j'' &= d_1 \cdot \left(\frac{p-1}{2} - i'\right) + d_2 \left(\frac{p-1}{2} - j'\right) = (d_1 + d_2) \left(\frac{p-1}{2}\right) - (d_1 \cdot i' + d_2 \cdot j') \\
&\equiv -(d_1 \cdot i' + d_2 \cdot j') \pmod{p-1} \\
&\equiv 0 \pmod{p-1}
\end{aligned}$$

here, we have that  $d_1, d_2$  are odd numbers and  $d_1 + d_2$  is even. And

$$i'' + j'' = \frac{p-1}{2} - i' + \frac{p-1}{2} - j' = p-1 - (i' + j') \leq \frac{p-1}{2}.$$

Now, let's assume that  $g_1 = \gcd(d_1, p-1) \geq 2$ . Let  $i = \frac{p-1}{g_1}, j = 0$  then

$$d_1 \cdot i + d_2 \cdot j \equiv 0 \pmod{p-1},$$

. and

$$i + j = \frac{p-1}{g_1} \leq \frac{p-1}{2}.$$

This completes the proof of the theorem. ■

*Example 1:* Let  $p = 5, d_1 = 2, d_2 = 3$ , we can find that  $2 \cdot 2 + 3 \cdot 0 \equiv 0 \pmod{4}$ , and  $i + j = 2 + 0 \leq 2$ ;

Let  $p = 7, d_1 = 2, d_2 = 3$ , we can find that  $2 \cdot 2 + 3 \cdot 1 \equiv 0 \pmod{6}$ , and  $i + j = 2 + 1 \leq 3$ ;

Let  $p = 11, d_1 = 3, d_2 = 7$ , we can find that  $3 \cdot 1 + 7 \cdot 1 \equiv 0 \pmod{10}$ , and  $i + j = 1 + 1 \leq 5$ ;

Let  $p = 11, d_1 = 7, d_2 = 9$ , we can find that  $7 \cdot 3 + 9 \cdot 1 \equiv 0 \pmod{10}$ , and  $i + j = 3 + 1 \leq 5$ .

## REFERENCES

- [1] A. Adolphson, and S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley-Waring, *Ann. Sci. Ecole Norm. Sup.*, 20(1987), 545-556.
- [2] F. Castro, R. Figueroa, and P. Guan, Improved Divisibility of Exponential Sums in One Variable and Some Consequences, arXiv:1401.4373v2.
- [3] O. Moreno and C. J. Moreno, Improvements of the Chevalley-Waring and the Ax-Katz theorems, *Amer. J. Math.* 1(1995), 241-244.
- [4] O. Moreno, K. Shum, F. N. Castro, and P. V. Kumar, Tight Bounds for Chevalley-Waring- Ax Type Estimates, with Improved Applications, *Proc. of the London Mathematical Society*, 88(2004), 545-564.
- [5] S. Sperber, On the p-adic Theory of Exponential Sums, *Amer. J. Math* 108(1986), 255-296.